

Department of Homeland Security

Information Analysis and Infrastructure Protection

"Unchecked buffer in Microsoft Internet Information Server (IIS)"

Advisory 03-005

March 17, 2003

SUMMARY:

A security vulnerability is present in a Windows component used by WebDAV, contains an unchecked buffer. Microsoft Windows 2000 and IIS Version 5.0 support the World Wide Web Distributed Authoring and Versioning (WebDAV) protocol.

IMPACT:

An attacker could exploit the vulnerability by sending a specially formed HTTP request to a machine running Windows 2000 server and IIS Version 5.0. The request could cause the server to fail or to execute code of the attacker's choice. The code would run in the security context of the IIS service which, by default, runs in the LocalSystem context.

DETAILS:

Microsoft Windows 2000 and IIS support the World Wide Web Distributed Authoring and Versioning (WebDAV) protocol. WebDAV, defined in RFC 2518, is a set of extensions to the Hyper Text Transfer Protocol (HTTP) that provide a standard for editing and file management between computers on the Internet. A security vulnerability is present in a Windows component used by WebDAV, and results because the component contains an unchecked buffer. Although Microsoft has supplied a patch for this vulnerability and recommends customers install the patch immediately, additional tools and preventive measures have been provided that customers can use to block the exploitation of this vulnerability while they are assessing the impact and compatibility of the patch.

RECOMMENDATIONS:

Users are encouraged to implement the patch for this vulnerability made available by Microsoft.

As an initial workaround Administrators can implement Microsoft's URL Scan tool to limit the lengths of URLs passed to the IIS system.

More information can be obtained from Microsoft's Security Bulletin MS03-007 and on workarounds from Knowledge Base document 816930

Update IDS signature files as relevant signatures become available.

Monitor FW, IDS, and other perimeter security devices for probes against port 80 and/or attempts to exploit this vulnerability.

Monitor information sources for additional alerts regarding possible attack activity.

Report any relevant activity (increased port 80 probing or activity, web server crashes, etc.) to your agency Incident Response Capability and FedCIRC.

Ensure that your incident response capability is prepared for a possible incident.

If successfully attacked, recognize that a system compromise may have taken place; take appropriate action based on your incident handling policy.

AFFECTED VERSIONS:

Microsoft IIS version 5.0 running on Windows 2000 servers is vulnerable.

CREDITS and REFERENCES:

Information from the following source was used in the preparation of this notice (URLs may be wrapped for readability):

Microsoft:

<http://www.microsoft.com/technet/security/bulletin/MS03-007>

The DHS/IAIP encourages system administrators heighten their awareness of network traffic during this period and for all individuals to report information concerning suspicious or criminal activity to their local FBI office, <http://www.fbi.gov/contact/fo/fo.htm> and to your homeland security watch office. Individuals may report incidents online at <http://www.nipc.gov/incident/cirr.htm>. Contact numbers for the DHS watch centers are: DHS/IAIP Watch and Warning unit at (202)323-3205, 1-888-585-9078, or nipc.watch@fbi.gov. DHS/NCC at (703) 607-4950 or ncs@ncs.gov. DHS/FedCIRC at (888) 282-0870 or fedcirc@fedcric.gov

The DHS/IAIP intends to update this alert should it receive additional relevant information, including information provided to it by the user community. No change to the Homeland Security Advisory Level is anticipated at this time.